CISSP – Certified Information Systems Security Professional

Days: *5*

Prerequisites: Students should have certifications in A+, Network+, or Security+, or possess equivalent professional experience. Students may have one or more of the following certifications or equivalent experience: MCSE, SCNP, CCNP, RHCE, LCE, CNE, SSCP, SANS, or GIAC.

Audience: Students pursuing CISSP training want to establish themselves as credible computer security professionals through a study of all 10 CISSP Common Body of Knowledge domains. Validating this knowledge is the goal of certification; therefore, students attending this training should also meet the requirements needed to sit for the CISSP certification exam. These include four years of direct professional work experience in one or more fields related to 10 CBK security domains, or a college degree and three years of experience. Check with (ISC)2 for the most up-to-date requirements. New certifications have emerged and will continue to emerge from (ISC)2, which may cause changes to base requirements.

Description: Welcome to Certified Information Systems Security Professional (CISSP)®. With your completion of the prerequisites and necessary years of experience, you are firmly grounded in the knowledge requirements of today's security professional. This course will expand upon your knowledge by addressing the essential elements of the 10 domains that comprise a Common Body of Knowledge (CBK)® for information systems security professionals. The course offers a job-related approach to the security process, while providing the basic skills required to prepare for CISSP certification.

OUTLINE:

LESSON 1 BECOMING A CISSP

LESSON 2 INFORMATION SECURITY GOVERNANCE AND RISK MANAGEMENT

- Fundamental Principles of Security
- Security Definitions
- Control Types
- Security Frameworks
- Risk Management
- Risk Assessment and Analysis
- Risk Analysis Approaches
- Information Classification
- Layers of Responsibility
- Security Steering Committee
- Security Governance

LESSON 3 ACCESS CONTROLS OVERVIEW

- Security Principles
- Identification, Authentication, Authorization, and Accountability
- Access Control Models
- Access Control Techniques and Technologies
- Access Control Administration
- Decentralized Access Control Administration
- Accountability
- Access Control Practices
- Threats to Access Control

LESSON 4 SECURITY ARCHITECTURE AND DESIGN

- Computer Security
- System Architecture
- Computer Architecture
- Operating System Architectures
- System Security Architecture
- Security Models
- Clark-Wilson Model
- The Orange Book and the Rainbow Series
- Common Criteria
- Certification vs. Accreditation
- Open vs. Closed Systems

LESSON 5 PHYSICAL AND ENVIRONMENTAL SECURITY

- Introduction to Physical Security
- The Planning Process
- Protecting Assets
- Internal Support Systems
- Perimeter Security

CISSP – Certified Information Systems Security Professional

LESSON 6 TELECOMMUNICATIONS AND NETWORK SECURITY

- Telecommunications
- Open Systems Interconnection Reference Model
- TCP/IP Model
- Types of Transmission
- Cabling
- Networking Foundations
- E-mail Services
- Intranets and Extranets
- Metropolitan Area Networks
- Wide Area Networks
- Remote Connectivity
- Wireless Technologies

LESSON 7 CRYPTOGRAPHY

- The History of Cryptography
- Cryptography Definitions and Concepts
- Types of Ciphers
- Methods of Encryption
- Types of Asymmetric Systems
- Message Integrity
- Various Hashing Algorithms
- Key Management
- Trusted Platform Module
- Link Encryption vs. End-to-End Encryption
- E-mail Standards
- Internet Security
- Attacks

LESSON 8 BUSINESS CONTINUITY AND DISASTER RECOVERY PLANNING

- Business Continuity and Disaster Recovery
- BCP Project Components
- Preventive Measures
- Recovery Strategies
- Insurance
- Recovery and Restoration
- Testing and Revising the Plan

LESSON 9 LEGAL, REGULATIONS, INVESTIGATIONS, AND COMPLIANCE

- The Many Facets of Cyber law
- The Crux of Computer Crime Laws
- Intellectual Property Laws
- Privacy
- Liability and Its Ramifications
- Procurement and Vendor Processes
- Investigations
- Ethics

LESSON 10 SOFTWARE DEVELOPMENT SECURITY

- Software's Importance
- Where Do We Place Security?
- System Development Life Cycle
- Software Development Life Cycle
- Secure Software Development Best Practices
- Software Development Models
- Change Control
- Programming Languages and Concepts
- Distributed Computing
- Web Security
- Web Application Security Principles
- Expert Systems/Knowledge-Based Systems
- Artificial Neural Networks
- Malicious Software (Malware)

LESSON 11 SECURITY OPERATIONS

- The Role of the Operations Department
- Administrative Management
- Assurance Levels
- Operational Responsibilities
- Configuration Management
- Media Controls
- Network and Resource Availability
- Mainframes
- Vulnerability Testing